DIRECTOR OF CENTRAL INTELLIGENCE
SECURITY COMMITTEE
COMPUTER SECURITY SUBCOMMITTEE

20 May 1983
DCISEC-CSS-M154

1. The One Hundred and Fifty-Fourth meeting of the Computer
STAT Security Subcommittee was held on 17 May 1983 at the
STAT McLean, VA. The following people attended:

STAT Chairman
STAT Executive Secretary
STAT CIA
CIA
Mr. Robert Graytock, Dept. of Justice
Mr. David Jones, DoE
STAT NSA
NSA
Mr. Carl Martz, Navy
Mr. James Studer, Army
Mr. Lynn Culkowski, Air Force
Mr. Lynn McNulty, Dept. of State
Mr. David Schenken, U.S. Secret Service
Mr. Gene Epperly, OSD
STAT SECOM Staff
STAT Chairman, SECOM
STAT
STAT SECOM
IC Staff
CIA (observer)

STAT 2. The meeting was visited by
STAT Chairman of the DCI SECOM, and
Inc., who has been contracted by the IC Staff to review the structure, policy, and standards of computer security across both the Intell and DoD communities.
STAT who was introduced to the Subcommittee by
STAT described the project as it is presently envisioned. It will include five parallel efforts, as follows:

(a) Policy - this would encompass "hand-shaking" agreements, such as MOU's between DoD and Intell., the definition of a standards-making and enforcement process, and the revision of DCID 1/16.

(b) Process - this area would address the certification/accreditation process, how support is provided to the field, and the assignment of responsibilities.

(c) Vulnerability/Threat/Risk - to include both generic and specific (e.g., case studies) vulnerabilities; will also address the need to obtain support from the Executive and Legislative branches.

(d) R&D - this aspect of the project will highlight R&D now being supported, push for more support for technology projects currently underway (e.g., DoDIIS, BLACKER), and identify technology which needs development.

(e) Action Agenda - this portion of the task would result in the setting of priorities, identifying standards to be developed, and identifying a phased approach for coming into compliance with standards/policy documents.

STAT [redacted] stated that she expected the project to be completed in approximately one year. However, she also noted that it would leave behind a legacy of an infrastructure as well as a five-year program and budget.

3. At the resumption of the regular business meeting, the Chairman stated his intent to have the Subcommittee support Dr.
STAT [redacted] fully. He noted, however, that, at the present time, the Subcommittee was only being asked to present briefings to Dr.
STAT [redacted] on the threat and the requirement for collection, and on the status of the DCID 1/16 rewrite. These will be given by the Executive Secretary and the Chairman.

STAT 4. The Chairman pointed out that, as a result of [redacted] project being initiated, the IC Staff has ordered that the rewrite of DCID 1/16 be put on hold. However, he has indicated to the SECOM his intention of completing the current efforts, at least insofar as capturing the results of the most recent discussions/work/agreements.

5. The next item of business was a discussion of the Subcommittee's R&D projects for FY83. The Chairman noted that we are funded at a level of $250K. The three tasks discussed in detail were:

(a) the Security Sign-On Device, installed at the Pentagon, with DIA as the COTR. The Chairman offerred a briefing and demonstration to whoever was interested in the device, which employs fingerprint identification technology;

(b) the Wang Alliance study, being COTR'ed by both State and CIA. The CIA member indicated that the technical performance of the LANL contractors was good, but that he has been dissatisfied with the reports to date;

(c) the threat estimate effort, being pursued by the Navy. The Navy member reported that the IR's are currently being reviewed.

6. The Executive Secretary presented a briefing on the status of the DCID 1/16 rewrite. The briefing reviewed the issues and agreements which led up to the most recent draft, and briefly outlined the structure of that draft. The primary purpose of the briefing, however, was to propose a restructuring of the regulatory section to allow telecommunications systems to fit smoothly into an overall structure. The viewgraphs of the briefing, as well as the proposed rewrite are enclosed. The views expressed by the membership were supportive of the ideas presented, although the observers from the CIA Telecommunications office expressed some concern with the applicability of the terminology to telecommunications systems.

7. The next meeting of the Computer Security Subcommittee
STAT was set for Tuesday, 21 June 1983 at 0930 at
STAT Members are asked to be prepared with specific comments on the proposed restructure of the regulatory section of DCID 1/16.

8. We note here the retirement of Mr. James Studer, who has served the Army, the Community, and the Subcommittee loyally for many years. Those who count him as a friend are legion, and they will miss his participation, while wishing him well in his retirement.

STAT

Executive Secretary

DCID 1/16

Yesterday, Today

and

Tomorrow

Current Document

"Security of Foreign Intelligence

in Automated Systems and Networks"

effective 4 Jan. 1983

Salient Characteristics

Policy Statement

- excluded telecommunications systems

Regulation

- defined three allowed modes of operation

Allowed Modes of Operation

A. Dedicated

- System exclusively dedicated to, and controlled for, the processing of one particular type of intelligence information.
- All users cleared to the level of the information being processed.

B. System High

- System operating with security measures commensurate with the highest classification and sensitivity of information being processed.
- All users cleared/access approved for all data in the system.

Allowed Modes of Operation (Con't)

C. Compartmented

- System processes two or more type of SCI, or, one type of SCI with other than SCI.
- System access secured to at least TOP SECRET, but all users not necessarily formally authorized access to all types of SCI on the system.
- All users cleared at least TOP SECRET.

Deficiencies of Current DCID

- Authorities/responsibilities not clear

- Overly rigid
    - 3 and only 3 modes of operation
    - underlying assumption too narrow
    - No allowance for new technology
    - No allowance for special environments

- Telecommunications exception
    - Confusing
    - Apparently inconsistent

Goals of Re-Write

- Better delineate responsibilities and authority
- Address shared systems
- Incorporate more flexibility
    - allow for variety of applications and environments
    - allow for engineering trade-offs
    - allow for technical innovation
    - allow for new modes
- Incorporate telecommunications

ISSUES

SCOPE

foreign intelligence vs. SCI

MODES

mandatory vs. recommendations

TELECOMMUNICATIONS

how stated?

Agreements

20 April 1982 mtg

- Scope is all foreign intelligence

  - Modes should not be mandatory; identify minimum requirements for commonly encountered environments, but allow for engineering trade-offs

    - Include an "expanded compartmented mode"

      - Identified an approach for dealing with telecommunications

Current Draft

Policy

- Define protection goals
- Define accreditation authority
    - single agency system
    - shared system
    - "concatenated" system
- Define responsibilities
- Administrative reports
- No telecommunications exception

Regulation

Define generic security requirements

- mandatory controls
- discretionary controls
- labelling
- accountability
- continuous protection

Prescribe minimum security requirements

- physical
- personnel
- administrative
- COMSEC
- TEMPEST

Regulation (Con't)

Define a set of security modes

- dedicated
- system high
- compartmented
- expanded compartmented

Remaining Issue:

Telecommunications

- Problem is political
- Not excluded,

Not included

Current Status

- Draft to SECOM 1 Feb 1983

- SECOM decisions

  - add telecommunications section
  - scope limited to SCI only

- Returned to CSS March 1983 for further development

A New Wrinkle:

A proposed re-structuring to solve the telecomunications problem

Sanitized Copy Approved for Release 2010/11/17 : CIA-RDP87T00623R000200070026-1

Define Five Modes of Operation

Dedicated

System High

Compartmented

Expanded Compartmented

Unlimited (i.e., full multi level)

Distributed Among Three General Classes of ADP Environments

User Class

Data Sharing Class

Process Sharing Class

Mode of Operation

- Defines a set of protection measures

  (hardware/software, physical, personnel, administrative)

Environment Class

- Defines the functionality afforded to the users of the ADP system

For each Environment Class, an allowable set of modes of operation are defined.

User Class

The ADP System provides general programming capability.

Allowable Modes

- Dedicated Mode
- System High Mode
- Compartmented Mode

Data Sharing Class

Does not provide software development facilities to the user;

Does provide data sharing and data management services.

Users allowed to read from, write to, alter, and manipulate globally-shared, system-maintained data.

Allowable Modes

- Dedicated Mode
- System High Mode
- Compartmented Mode
- Expanded Compartmented Mode

Process Sharing Class

ADP system provides the capability to execute pre-defined processes which run in user's behalf;

Does not support general programming;

Data not shareable at user's discretion.

(e.g. Pure Comm. Processor, Transaction Processors, Terminal Concentrator, security "filter")

Allowable Modes

- Dedicated Mode
- System High Mode
- Compartmented Mode
- Expanded Compartmented Mode
- Unlimited Mode

Unlimited Mode

One or more types of SCI along with collateral (non-SCI)

System access is provided to users of arbitrary clearance (incl. uncleared)

System designed, engineered, and configured specifically to operate in Unlimited Mode.

NFIB member involved in the decision to develop and implement system operation in the Unlimited Mode.

All system software developed in controlled environment by cleared programmers.

ADVANTAGES

- Telecommunications fits smoothly into an overall, consistent framework
- No need to allow nebulously-defined "engineering latitude"

DISADVANTAGES

Definitions not clear enough; need to describe fundamentals.